

**UNITED STATES DISTRICT COURT
DISTRICT OF NEW HAMPSHIRE**

IN THE MATTER OF THE SEARCH)	
OF A BLACK DELL INSPIRON)	
LAPTOP COMPUTER)	
LOCATED AT BEDFORD POLICE)	Case No. 1:20-mj- 146-01-DL
DEPARTMENT, 55 CONSTITUTION)	
DRIVE, BEDFORD, NH)	

**AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT**

I, Shawn Serra, a Special Agent with the United States Department of Homeland Security, Immigration and Customs Enforcement, Homeland Security Investigations, being duly sworn, do depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant authorizing a search of the black Dell Inspiron 15 laptop computer described in Attachment A believed to be used by Matthew Dion currently located in secure storage at the Bedford Police Department, 55 Constitution Drive, Bedford, New Hampshire ("the Device"). I seek authority to search the Device and extract from it electronically stored information that constitutes evidence, fruits, and instrumentalities of criminal violations which relate to the possession and attempted production of child pornography, as described in Attachment B.

2. I have been employed as an HSI Special Agent since June of 2005, and am currently assigned to the Manchester, New Hampshire, Resident Office. I graduated from the University of Massachusetts, Lowell, Massachusetts, with a Bachelor of Science Degree in Criminal Justice. In 2003, I graduated from the University of Massachusetts, Lowell, Massachusetts, with a Master of Arts Degree in Criminal Justice. I have also received training in

the areas of child sexual exploitation including violations pertaining to possession and production of child pornography by attending a twenty-three-week training program at the Federal Law Enforcement Training Center (FLETC) in Glynco, Georgia. As part of my duties, I have observed and reviewed examples of child pornography (as defined in 18 U.S.C. § 2256) in various forms of media, to include digital/computer media. During the course of this investigation, I have also conferred with other investigators who specialize in computer forensics and who have conducted numerous investigations which involved child sexual exploitation offenses.

3. I am a "Federal law enforcement officer" within the meaning of Federal Rule of Criminal Procedure 41(a)(2)(C), that is, a government agent engaged in enforcing the criminal laws and duly authorized by the Attorney General to request a search warrant.

4. The information contained in this affidavit is based on information conveyed to me by other law enforcement officials, and my review of records, documents and other physical evidence obtained during this investigation. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have set forth all material information but have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that evidence, fruits, and instrumentalities of violations of the Specified Federal Offenses are presently located on the Device.

5. I submit that the facts set forth in this affidavit establish probable cause to believe that violations of 18 U.S.C. §§ 2251 (production of child pornography and attempted production of child pornography) and 2252(a)(4)(B) (possession of child pornography) have been committed by Matthew Dion and that there is probable cause to believe that evidence and fruits,

and instrumentalities of violations of 18 U.S.C. §§ 2251 and 2252(a)(4)(B), as set forth below, will be found on the premises.

RELEVANT STATUTES

6. 18 U.S.C. § 2251 prohibits the production and attempted production of child pornography. 18 U.S.C. § 2252 prohibits a person from knowingly possessing or accessing sexually explicit images (child pornography) with the intent to view them, as well as transporting, receiving, distributing or possessing in interstate or foreign commerce, or by using any facility or means of interstate or foreign commerce, any visual depiction of minors engaging in sexually explicit conduct (i.e., child pornography). The following definitions apply to this Affidavit and Attachment B:

a. **“Child Exploitation Material”**, as used herein, includes known or identified victims depicted in a non-sexually explicit manor (various stages of undress, from the back, face only, etc.), non-nude minors (clothed in sexually provocative poses, wearing sexually suggestive clothing or lingerie, etc.), of indeterminate age (post-pubescent, sexually explicit, but unable to say for certain that they are under 18 years of age).

b. **“Child Pornography”**, as used herein, is defined in Title 18 United States Code § 2256 (any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct).

c. **“Minor”** means any person under the age of eighteen years. See 18 U.S.C. § 2256(1).

d. **“Sexually explicit conduct”** means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any person. See 18 U.S.C. § 2256(2).

PROBABLE CAUSE

7. On or about April 19, 2020, the Bedford, New Hampshire, Police Department was contacted by a representative of an organization that facilitates foreign exchange students traveling to the United States and residing with American host families. The program partners with a high school in Nashua, New Hampshire. According to the caller, a sixteen-year-old student (“Minor Victim” or “MV”) reported to his family and to the exchange program that he believed a member of his host family had been recording him while he showered. After receiving the report, the exchange program contacted the Bedford Police Department.

8. Two Bedford Police officers responded to the home of Matthew Dion (“DION”), the host family in Bedford, New Hampshire. Officers spoke to MV outside the home. MV was interviewed again on or about April 28, 2020, in an interview with the Child Advocacy Center. In the two interviews, MV reported that he found what he believed to be a camera hidden inside a device that looked like a pen in the bathroom that he used in the residence. He said that the pen was frequently in the bathroom and located in different places but that he previously did not think much of it. On or about April 18, 2020, he entered the bathroom and noted the trash can had been pulled forward. The trash was full and there was an empty toilet paper roll placed

upright. Inside the empty toilet paper roll, the pen was situated upright and pointed directly toward the toilet. At that time, MV thought it was strange but did not investigate further. The day of the report, he entered the bathroom and the trash was still full, but the pen had been removed and was now placed on the vanity. MV entered the shower and noticed a small tubular item wrapped in black tape propped against a razor. He examined it and noticed a small cut out in the tape that looked like a glass lens. He was concerned as he believed it was a camera and got out of the shower immediately.

9. He then examined the pen. He took it apart and noticed a USB connector inside it and what appeared to be a camera lens. After MV found what he believed to be a camera, he went to his room to contact his family. His parents encouraged him to go back to the bathroom to double check and document the items. He went back to the bathroom minutes after leaving and crossed paths with DION. When he went into the bathroom, both items had been removed. According to MV, DION frequently went into the bathroom before and after MV took showers.

10. While the police officers were at the residence that night, another minor child living in the residence stated that he had also seen something consistent with that pen in the bathroom. Officers searched the bathroom and did not find the pen. When questioned about it, DION said he had received a pen with a USB attached to it from work and provided it to officers. MV looked at the pen and said it was not the one he had seen in the bathroom. MV searched the internet and found a photograph of a pen with a hidden camera in it that he said was consistent with the one he had seen in the bathroom. MV left the house that evening.

11. On or about April 28, 2020, the Honorable Mark S. Derby of the 9th Circuit District Division Merrimack Court, authorized a warrant to search DION's residence in Bedford, the person of Matthew Dion, and his vehicles, for evidence of violation of privacy, N.H. Rev.

Stat. 644:9. The warrant was executed that same day. During the search, officers seized various items including a Micro SD card from DION's vehicle. The Micro SD card is labeled "made in China."

12. While the search warrant was being executed, DION agreed to speak with investigators. When asked about the pen described by MV, DION said that he was totally unaware of it. Officers did not find anything resembling a hidden camera during the search of the residence. When questioned about whether he owned any electronic storage devices, he told investigators that there were two SD cards in his car, one that had fallen under the seats and one that was in the SD player. He said they would have music on them.

13. Officers found two SD cards in DION's vehicle both of which were between or under the seats. Officers showed the Micro SD card to DION and he said he did not recognize it and said he had never seen it before. He suggested someone must have dropped it in his vehicle. He said he did not know who that could be because he was the only person to use the vehicle.

14. Officers later searched the Micro SD card. On the Micro SD card, officers found images that appeared to be taken in the bathroom that MV used. A still frame from what appears to have originally been a video clip seems to show a man setting up the recording device. The image only captures from his eyebrows to the top of his head but the part of the man's head that is visible is consistent with DION. Also on the device, investigators found images that appeared to be taken of MV using the bathroom. A forensic examiner was able to determine that the SD card was reformatted on or about April 21, 2020. This is consistent with someone attempting to delete items off of the device on that date. I note that this is just a few days after the Bedford Police spoke to DION about MV's allegations.

15. After an initial review of the devices, officers received a second search warrant. On May 15, 2020, United States Magistrate Judge Andrea K. Johnstone issued a warrant to search the Micro SD card and other devices for evidence of production of child pornography. Officers then searched the Micro SD card, and found, among other things, an image with the following MD5 hash value: 8983 4f0a 98d9 2a9a 6152 0569 46d4 f45c. The image depicts a naked male getting out of the shower. The focal point of the image is on the male's penis, which is fully exposed. The image is one of a series of images that appear as if they were originally part of a video, depicting the male in and getting out of the shower.

16. On or about June 18, 2020, officers showed MV a sanitized version of the image. MV identified himself in the image and said that it was taken as he was getting out of the shower in the bathroom in his host family's house in Bedford, while he was residing there as an exchange student. MV arrived at the residence in August 2019 and left in April 2020.

17. On or about June 22, 2020, Matthew Dion was charged by complaint with one count of producing child pornography.

18. On or about July 23, 2020, a member of the Bedford Police Department contacted the adult stepson of Matthew Dion ("Witness 1"). Witness 1 told officers that he just learned of DION's charges. He said that DION provided him with a laptop about two months prior and that he wanted to turn it over to police. He said he did not know why DION provided him with the laptop and thought it was odd. Witness 1 had used the laptop since then for internet streaming and browsing but did not save any pictures to the laptop. Witness 1 also stated that growing up, he recalled waking up at night to find DION in his room staring at him and added that sometimes when he would shower, DION would be in the bathroom standing there when he got out.

19. The Device is currently located in an evidence locker at the Bedford Police Department. I know that it has been stored in a manner that has prevented tampering or alteration since it has been seized. Even if DION erased content from the computer prior to providing it to his stepson, I know that forensics experts can recover deleted items from computers. I therefore believe that there is probable cause to search the Device for evidence of the crimes discussed herein.

**CHARACTERISTICS COMMON TO INDIVIDUALS WHO POSSESS OR PRODUCE
CHILD PORNOGRAPHY**

20. Based on my previous investigative experience related to child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I know there are certain characteristics common to individuals who view and/or possess, receive, and/or produce images of child pornography:

- a. Individuals who possess, receive, and/or produce child pornography may receive sexual gratification, stimulation, and satisfaction from contact with children, or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media, or from literature describing such activity. Individuals who have a sexual interest in children or images of children typically retain such images for many years.
- b. Likewise, individuals who possess, receive, and/or produce child pornography often maintain their child pornography images in a digital or electronic format in a safe, secure and private environment, such as a computer or smartphone. These child pornography images are often maintained for several years and are kept close by, to enable the individual to view the child pornography images, which are valued highly.

c. Individuals who possess, receive, and/or produce child pornography also may correspond with and/or meet others to share information and materials, rarely destroy correspondence from other child pornography distributors/possessors, conceal such correspondence as they do their sexually explicit material, and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography. Forums, such as chat rooms, bulletin boards, newsgroups or IRC chat rooms have forums dedicated to the trafficking of child pornography images.

21. I know, based on my training and experience, that people who have a demonstrated sexual interest in children and child pornography often maintain collections of images of child pornography. I am therefore requesting authority to search the Device for evidence of child pornography or any communication involving MV or other foreign exchange students who have lived with DION, evidence of child erotica or child pornography created by the defendant, sexually explicit images of children, evidence of placement of hidden cameras, and any other child pornography and evidence relating to the production, possession, and distribution of any child pornography or child exploitation material.

22. I also know that people who possess or produce child pornography frequently use computers, computer technology, and the Internet. Computers basically serve five functions in connection with child pornography: production, communication, distribution, storage, and social networking. With digital cameras, images of child pornography can be transferred directly onto a computer; in addition, the use of commercially available software and devices also allows for the conversion and transfer of other forms of visual media into various digital and electronic media formats.

23. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. The size of the electronic storage media (commonly referred to as the hard drive) used in home computers has grown tremendously within the last several years. These drives can store thousands of images at very high resolution.

24. As with most digital technology, communications made from a computer are often saved or stored on that computer. Storing this information can be intentional, for example, by saving an e-mail as a file on the computer or saving the location of one's favorite websites in "bookmarked" files. Digital information can also be retained unintentionally. Traces of the path of an electronic communication may be automatically stored in many places, such as temporary files or ISP (Internet Service Provider) client software, among others. In addition to electronic communications, a computer user's Internet activities generally leave traces in a computer's web cache and Internet history files. A forensic examiner often can recover evidence that shows whether a computer contains peer-to-peer software, when the computer was sharing files, and some of the files that were uploaded or downloaded. Computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted, or viewed via the Internet. Electronic files downloaded to a hard drive can be stored for years at little or no cost. Even when such files have been deleted, they can be recovered months or years later using readily available forensic tools. When a person "deletes" a file on a home computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space -- that is, in space on the hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space -- for long periods of time before they are overwritten. In addition, a computer's operating

system may also keep a record of deleted data in a “swap” or “recovery” file. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or “cache.” The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user’s operating system, storage capacity, and computer habits.

25. I also know that electronic devices store evidence that can inform investigators who used the computer, when, and how it was used.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

26. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

27. There is probable cause to believe that things that were once stored on the Device may still be stored there, for at least the following reasons:

28. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

29. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

30. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

31. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

32. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Device was used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence might be on the Device because:

33. Data on a storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).

34. Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.

35. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

36. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

37. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

38. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the Device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the Device to human inspection in order to determine whether it is evidence described by the warrant.

39. *Manner of execution.* Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

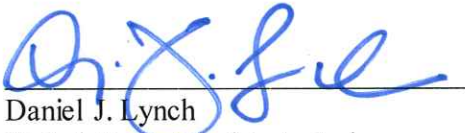
40. Based on the foregoing, there is probable cause to believe contraband, evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 2251 (sexual exploitation of children and attempt) and/or 18 U.S.C. § 2252(a)(4)(B) (possession of child pornography) will be found on the Device described in Attachment A. I respectfully request that this Court issue a search warrant for the Device, authorizing the seizure and search of the items described in Attachment B.

/s/ Shawn Serra
Special Agent Shawn Serra
Department of Homeland Security
Homeland Security Investigations

The affiant appeared before me by telephonic conference on this date pursuant to Fed. R. Crim. P. 4.1 and affirmed under oath the content of this affidavit and application.

Date: July 31, 2020

Time: 9:00 am


Daniel J. Lynch
United States Magistrate Judge
District of New Hampshire

ATTACHMENT A

The property to be searched includes a black Dell Inspiron 15 laptop computer with serial number 1M585C2 currently located in the custody of the Bedford Police Department, 55 Constitution Drive, Bedford, New Hampshire.

This warrant authorizes the forensic examination of the Device for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

All records on the Devices described in Attachment A that relate to violations of 18 U.S.C. § 2251 (production of child pornography and attempted production of child pornography) and/or 18 U.S.C. § 2252(a)(4)(B) (possession of child pornography) including:

1. Any and all notes, documents, records, or correspondence, in any format and medium (including, but not limited to, e-mail messages, chat logs, electronic messages, or other digital data files) pertaining to the production and possession of child pornography as defined in 18 U.S.C. § 2256(8) or to the possession of visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2).
2. In any format and medium, all originals, computer files, and copies of child pornography as defined in 18 U.S.C. § 2256(8), child exploitation material, visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2), images or videos of children showering or using the bathroom, or child erotica.
3. Any and all diaries, address books, names, and lists of names and addresses of individuals who may have been contacted by the owner of the Device for the purpose of receiving child pornography as defined in 18 U.S.C. § 2256(8) or visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2).
4. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, e-mail messages, chat logs, electronic messages, and other digital data files) concerning contact, communications, and the relationship between DION and MV or other foreign exchange students.
5. Any and all notes, documents, records or correspondence, in any format or medium concerning contact between DION and any minor children under the age of eighteen other than his own children.
6. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, e-mail messages, chat logs, electronic messages, and other digital data files) concerning child pornography or membership in online groups, clubs, or services that provide or make accessible child pornography to members.
7. Any and all records, documents, invoices and materials, in any format or medium (including, but not limited to, e-mail messages, chat logs, electronic messages, and other digital data files) that concern online storage or other remote computer storage, including, but not limited to, software used to access such online storage or remote computer storage, user logs or archived data that show connection to such online storage

or remote computer storage, and user logins and passwords for such online storage or remote computer storage.

8. Any evidence of use or ownership of hidden camera devices.

9. Any and all documents, records, or correspondence, in any format or medium (including, but not limited to, e-mail messages, chat logs, electronic messages, and other digital data files), pertaining to use or ownership of the Device described above.

10. Any and all documents, notes, and any other records reflecting personal contact and any other activities with minors visually depicted while engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2).

As used above, the terms “records” and “information” include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.